PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-313640**
(43)Date of publication of application : **09.11.2001**

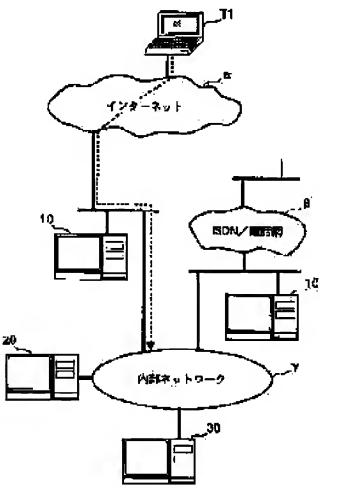
(51)Int.Cl. **H04L 12/24**
H04L 12/26
G06F 13/00
H04L 12/22

(21)Application number : **2000-133494**
(22)Date of filing : **02.05.2000**

(71)Applicant : **NTT DATA CORP**
(72)Inventor : **BABA TATSUYA**
YAMAOKA MASATERU
KOKUBO KATSUTOSHI
MATSUDA YOSHIYUKI

(54) METHOD AND SYSTEM FOR DECIDING ACCESS TYPE IN COMMUNICATION NETWORK AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an illegal access detection system capable of detecting illegal accesses of various patterns including an unknown method.
SOLUTION: The latest access policy of a site to be a management object is acquired from a management server 20 and held. Packets addressed to the site are acquired among packets circulated in a network, and packets suitable for the access policy and packets unsuitable for the access policy are sorted amount the acquired packets. When a packet unsuitable for the policy is selected, the packet is specified as a packet having possibility of being an illegal access and notified to the management server 20 in order to change an access condition for removing an access based on the specified packet.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－313640
（P2001－313640A）
(43)公開日　平成13年11月９日(2001.11.9)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　12/24		Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
12/26		Ｈ０４Ｌ　11/08		５Ｋ０３０
Ｇ０６Ｆ　13/00	３５１	11/26		９Ａ００１
Ｈ０４Ｌ　12/22				

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

(21)出願番号　特願2000－133494(P2000－133494)

(22)出願日　平成12年５月２日(2000.5.2)

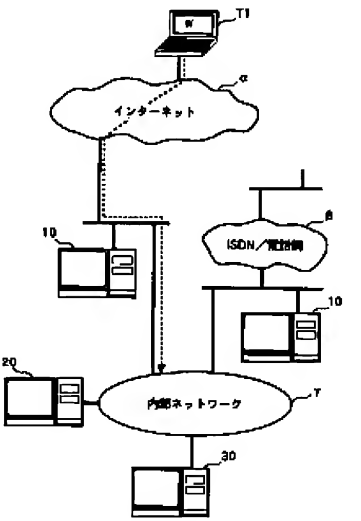
特許法第30条第１項適用申請有り　平成12年３月14日～３月16日　社団法人情報処理学会主催の「第60回（平成12年前期）全国大会」において文書をもって発表

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　局場　達也
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　山岡　正輝
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100099324
弁理士　鈴木　正剛

最終頁に続く

(54)【発明の名称】　通信ネットワークにおけるアクセス種別を判定する方法及びシステム、記録媒体

(57)



1 2

10

20

30

40

50

(3)

3

4

P.A Porras and P.G Neumann. EMERALD:Event mo nitoring enabling responses to anomalous live dist urbances. In Proceeding of the 20th NationalInform ation Systems Security Conference. pp.353-365.Oct. 1997

10

20

Cisco Sy
stems, Inc Cisco Secure IntrusionDetection Sy
stem Internet Secur
ity Systems, Inc RealSecure

30

H.S.Javits and A.Valdes.The SRI IDES Statist ical Anomaly Detector.In Proceedings of the IEEE S ymposium on Security and Privacy,May 1991

IDS M OFS99 15 A199 27 pp 39
46 July 1999

WWW
world wide web DNS domain name s
40 ervice

50

(4)

5 6

10

20

30

40

50

(5)

7 8

10

20

30

ISDN MAC Media Access Contro

40

File Transfer Protocol

50

(6)

IP TCP UDP ICMP
HTTP FTP SMTP DNS TELNET

IP
TCP UDP ICMP
HTTP SMTP DNS

IP

HTTP URL SMTP

File Transfe
r Protocol

(7)

11 *12*

URL

WWW

10

a. b. c. d

ht

IP IP tp tcp

a. b. c. e

smtp tcp

20

WWW HTTP

URL

WWW HTTP

URL

30 Index html whatsnew pro

ducts profile

40

SMTP

URL WWW

SMTP SMTP IP

SMTP

WWW *50*

HTTP

HTTP IP TC

P HTTP HTTP Yes

IP

IP

IP IP

IP

TCP IP HTT

P

HTTP

HTTP

RFC1945 RFC2068

HTTP

GE

T POST

GET Request URL HTTP 1.1 1.1

GET Request URL HTTP 1.0 1.0

GET Request URL

Request URL

URL

HTTP 1.0 HTTP 1.1

TCP UDP

"Req

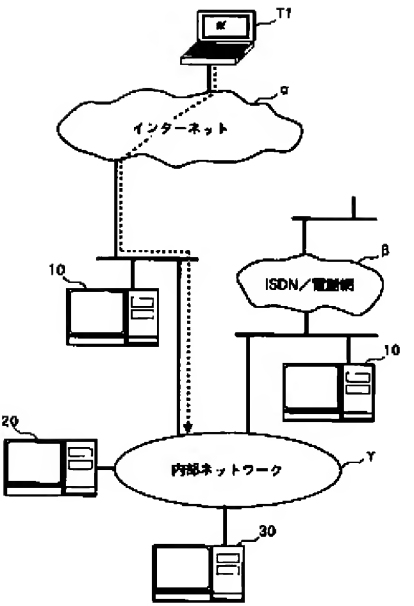
uest-URL"

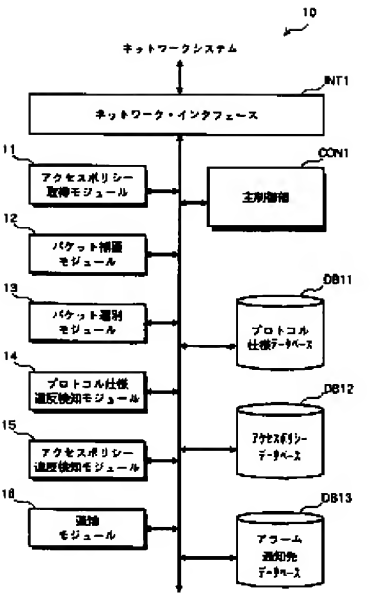
No

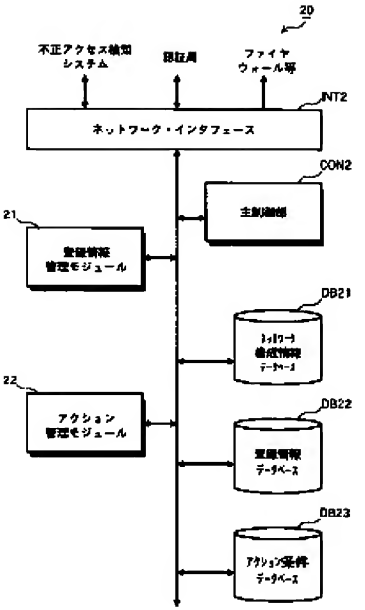
15 16

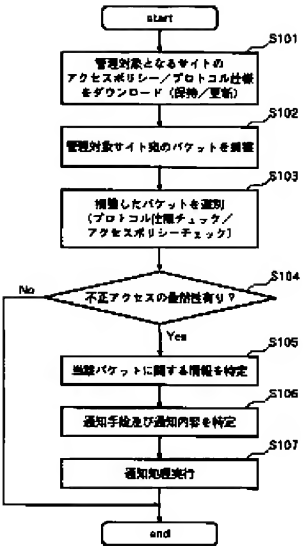
10

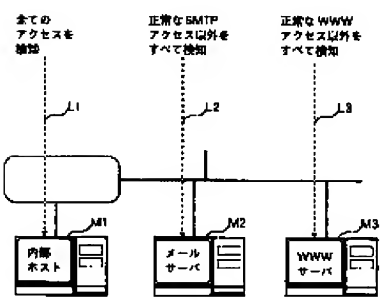
20 ISDN



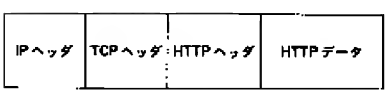








送信元アドレス	宛先アドレス	プロトコル	ユーザ名	プロトコル特有の条件
すべて	a.b.c.d	http／tcp	ANY	公開するファイル ／index.html ／whatsnew／＊ ／profile／＊ ・・・・・・・・・
すべて	a.d.c.e	smtp／tcp	ANY	使用するメールアドレス ＊＊＊＊@a. co. jp ＊＊＊＊@b. co. jp 許可するコマンド MAIL, DATA



通知手段	通知先	通知内容	使用
電子メール	postmaster@a.co.jp	不正アクセスが発生しました 送信元：　宛先：　プロトコル：	○
ポケベル	03－1234－5678	不正アクセスが発生しました 送信元：　宛先：　プロトコル：	×
コンソール		不正アクセスが発生しました 送信元：　宛先：　プロトコル：	○
・・・	・・・・・・・・・・	・・・・・・・・・・・・・・・・・・	

(a)

プロトコル仕様違反検知モジュール	チェック項目	チェック結果
ＩＰ	IPヘッダ長	正常
	IP全体長	正常
	フラグメント	正常
TCP	TCPヘッダ長	正常
ＨＴＴＰ	リクエスト形式	違反

(b)

アクセスポリシー違反検知モジュール	チェック項目	チェック結果
ＩＰ	宛先アドレス	正常
	送信元アドレス	正常
TCP	宛先ポート	正常
	送信元ポート	正常
ＨＴＴＰ	URL内容	違反

(72)

(72)

(5B089 GA11 GA21 GB02 HA03 HA06
HA10 JA22 JA31 JB22 KA17
KB04 KB06 KB13
5K030 GA15 HB16 HB18 HC01 KA04
KA13 LA08 LB02 LD19 LD20
9A001 CC06 JJ14 JJ25 LL03